短期大学における情報セキュリティポリシー（案）

平成17年4月15日
運営問題委員会

情報セキュリティポリシーの構成

情報セキュリティポリシーとは、本学が保有する情報資産（ネットワーク上を流通する情報やコンピュータ及びネットワークなどの情報システム）に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティ基本方針

1. 目的

本学では、学術研究、教育活動、大学運営業務等において、情報化を推進してきている。これらの情報化の推進と共に、情報資産の重要性も増してきている。このため、学内外の情報セキュリティを損ねる加害行為を抑止し、情報資産の安全性を確保し、そして、学内外の教育者、研究者等からの安全性の信頼を得ることも必要不可欠となってくる。

このことから、本学の情報資産の機密性、完全性及び可用性を維持するための対策を整備するため、情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

2. 定義

① コンピュータ
ハードウェア、及びソフトウェアで構成するコンピュータ、及び周辺機器ならびに記録媒体をいう。

② 磁気ディスク等
コンピュータに使用される磁気ディスク、テープ、光ディスクその他これらに類する記憶媒体をいう。

③ 情報管理室
サーバー、学生情報、成績情報、入試情報などを扱うコンピュータを設置している部屋をいう。

④ ネットワーク
コンピュータを相互に接続するための学内通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行なう仕組みをいう。

⑤ 情報システム
ネットワーク機器（ルータ、ファイアフォール、ハブ、ケーブルなど）、サーバー、パソコン、基本ソフトウェア、応用ソフトウェア、システム設定情報（パスワードファイル等）、記録媒体（MO、FD）、システム構成図、持ち込まれたノートパソコンなどの総称。
情報システムに記録される情報とは、アクセス記録（ログ）、文書及び図面等の電磁的記録を指す。

⑥ 情報資産
情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称。電磁的に記録された情報すべてを含む。

⑦ 情報セキュリティ
情報資産の機密性、完全性、及び可用性を維持することとする。
機密性とは、情報にアクセスすることが認可された者だけがアクセスできることを確実にすることとする。
完全性とは、情報及び処理方法の正確さ及び完全である状態を安全防護することとする。
可用性とは、許可された利用者が、必要なときに情報にアクセスできることを確実にすることとする。別名をアベイラビリティ（availability）といい、「有効性」の意味だが、日本語での訳語として「可用性」を当てる。コンピュータ業界得意の造語であり、システム全体をダウンさせることなく、継続稼動させる能力をいう。

⑧ 脅威
自然災害、機器障害、悪意のある行為など、損失を発生させる直接の要因のこととする。
⑨ 脆弱性
建物の構造上の欠陥、定期点検の不備、情報セキュリティ規定・要員教育の不備など脅威を発生し易くさせる要因、脅威を増加させる原因(脆さ、弱点)のこととする。

3. 情報セキュリティポリシーの位置付け
情報セキュリティポリシーは、本学の情報セキュリティ対策について、総合的・体系的かつ具体的にまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

4. 情報セキュリティポリシーの対象範囲
情報セキュリティポリシーの対象範囲は、本学の情報資産及び情報資産に接するすべての教職員(非常勤教職員、派遣社員を含む)および学生とする。

5. 教職員の責務
教職員は情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

6. 管理体制
本学の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

7. 情報資産の分類
情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行なうものとする。

8. 情報セキュリティ対策
本学の情報資産を脅威から保護するため、以下の情報セキュリティ対策を講ずる。
① 物理的セキュリティ対策
情報システム設置場所について、安全性を保ち、不正な立ち入りなどから保護するため、入退室や機器管理上の対策を講じる。
② 人的セキュリティ
全構成員に対して、情報セキュリティポリシーを周知徹底させるとともに、各人がどのような権限と責任を持っているかを明らかにし、情報セキュリティを確保するための啓発活動や教育を講じる。
③ 技術セキュリティ
学外または学内からの不正なアクセスから情報資産を適切に保護するため、情報ネットワークのアクセス制御・管理に必要な対策、コンピュータウイルス対策等を講じる。

9. 情報セキュリティ対策基準の策定
情報セキュリティ対策を行なう上で、教職員が遵守すべき事項や判断等の基準を統一して行なうために必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

10. 情報セキュリティ実施手順の策定
情報セキュリティポリシーを確実に実施していくためには、個々の情報資産に対する対策の手順を具体的に定めておく必要がある。情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

11. 評価・見直し
情報セキュリティポリシーに定める事項及び情報セキュリティ対策についての評価、情報システム

の変更、新たな脅威など情報システムに関する状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。

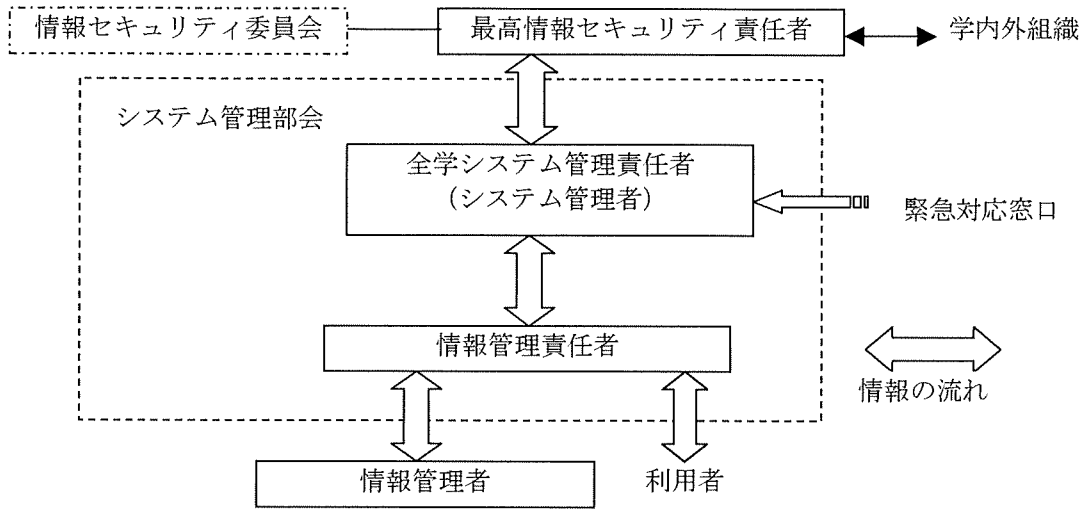
情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針に従い、本学の情報資産を保護・運用するために遵守すべき事項を記載したものである。

1. 管理体制

情報セキュリティ管理については、以下の体制とする

管理運用組織の構成



① 最高情報セキュリティ責任者
- 全学の情報セキュリティに関する総括的な意思決定と、学内、他の組織および学外に対する責任を負う。

② 全学システム管理責任者
- 全学の情報システム管理の実施に関し、緊急時の連絡など、総括的な対応に当たり、最高情報セキュリティ責任者を補佐する。

③ 情報管理責任者
- 情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う課（これに準ずるものを含む）に情報セキュリティに関する権限及び責任を有する情報管理責任者を置き、情報資産を取り扱う課、または学科の代表者をもってこれに充てる。
- 情報管理責任者は、所轄する情報資産に係る情報セキュリティ実施手順の作成・維持・管理を行うとともに、定められている事項について教職員に実施及び遵守させなければならない。
- 情報管理責任者は、使用する情報資産の機器や記録媒体について、第三者に使用させること、又は許可なく情報を閲覧させることがないように、適切な処置を施さなければならない。

④ 情報管理者
- 情報資産を現場で取り扱う担当者。

⑤ 情報セキュリティ委員会
- 情報セキュリティポリシーの策定、改訂を行なう。

・ その他、情報セキュリティに関する重要事項の決定を行なう。

3. 情報の分類と管理

① 情報の分類

対象となる全ての情報は、次の重要性分類に従って分類する。

(1)重要性分類Ⅰ

・ 本学受験志願者、及び本学の学生個人の成績情報など
・ 漏洩した場合、本学に対する信頼を著しく害するおそれのある情報
・ 滅失し、または棄損した場合、その復元が著しく困難となり、大学運営の円滑な執行を妨げる恐れのある情報
・ 情報システムに関わるパスワード及びシステム設定情報

(2)重要性分類Ⅱ

・ 脅威にさらされた場合に実害を受ける危険性は低いが、大学事務の執行及び、大学教育において重要性は高いと評価される情報
・ 公開されると大学業務、教育の円滑な執行に著しい障害を生ずる恐れのある情報

(3)重要性分類Ⅲ

上記以外の情報

② 情報の管理方法

(1)情報の管理及び取り扱い

・ 情報の重要性分類に従い、パスワード等によるアクセス制限及び、必要に応じては暗号等による通信内容の秘匿を行わなければならない
・ 重要性分類Ⅰの情報の不用意な複製や、送付・送信は行ってはならない
・ 教職員は、業務上必要な場合には、情報管理責任者の許可を得た上で情報の複製・送付・送信を行わなければならない

(2)記録媒体の管理

・ 重要性分類Ⅰ・Ⅱの情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない

(3)記録媒体の処分

・ 記録媒体が磨耗等により不要となった場合は、当該媒体に記録されている情報性分類Ⅰ・Ⅱの情報をいかなる方法によっても復元できないように消去等を行った上で廃棄しなければならない

4. 物理的セキュリティ

① 入退室の管理

情報管理者は、重要性分類Ⅰ・Ⅱの情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所への入退室管理について必要な措置を講じなければならない。

② 教職員の情報システムの機器管理

教職員は研究室、事務室が不在となる場合には、施錠をするなど部外者の侵入を防ぐ措置を講じなければならない。

③ 機器等の搬入・搬出

・ コンピュータ室等へ機器等を搬入・搬出する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、教職員による確認を行わなければならない。
・ 機器等の搬入・搬出には、教職員が立ち会う等の必要な措置を講じなければならない。

④ 電源

停電及び電圧異常などによりデータ等が破壊され、業務処理に支障を来たす恐れのある情報システム等の機器の電源は、当該機器を適切に停止するまでの間に必要な電力を供給する容量の予備電源を備え付ける等の措置を講じなければならない。

⑤ 配線

配線は、傍受又は損傷等を受けることがないよう可能な限り必要な措置をほどこさなければな

らない。

4. 人的セキュリティ

① 利用者

- 教職員は、情報セキュリティポリシーを遵守しなければならない。学生も情報システム利用者の一員として、情報セキュリティを維持する義務を有する。
- 教職員は、情報セキュリティ実施手順を遵守して、利用しなければならない。さらに、システム管理者からセキュリティ維持管理のために協力を依頼された場合には従わねばならない。
- 教職員は、情報セキュリティ実施手順について不明な点、遵守することが困難な点がある場合には、速やかに情報管理責任者に相談し、指示を仰がなければならない。

② 教育研究上の利便性の配慮

- 情報セキュリティ対策について教育研究上の利便性を著しく損なう点、遵守することが現実的に困難な点については、最高情報セキュリティ責任者またはシステム管理者に対して、ポリシーおよび実施手順の改善を求めることができる。
- 教職員および学生は、システム管理者の許可を得ずに情報端末等を研究室および、教室外に持ち出してはならない。ただし、モバイル端末は、教育研究上の利便性を考慮し、その利用者の管理責任において、これを持ち出せるよう配慮する。
- 教職員および学生以外の者(来学者)に学内の情報システム(公共情報端末や情報コンセントを含む)を一時的に使用させる場合においては、その利用者が守るべきポリシーを定め、これを遵守させるよう適切な措置を施さなければならない。

③ 教育・研修

- 情報セキュリティ委員会は、情報管理責任者向けの研修を開催しなければならない。
- 情報セキュリティ委員会は、情報管理責任者が、情報管理者に行う研修プログラムの実施に必要な措置を施さなければならない。
- 情報セキュリティ委員会は、システム管理者等が行う教職員向けのポリシーに関する研修の支援をしなければならない。また、教職員が行う学生向けのポリシーに関するオリエンテーションまたは講義に協力しなければならない。
- すべての教職員および学生は、研修会や説明会、または講義等を通じ、ポリシーおよび実施手順を理解し、情報セキュリティ上の問題が生じないように努めなければならない。

④ 事故・障害の報告

- 教職員および学生は、情報セキュリティに関する事故、情報システムの不審な動作、公開情報の改ざん、システム上の障害および誤動作を発見した場合には、全学システム管理責任者かシステム管理者、または情報管理責任者に直ちに報告しなければならない。
- 情報管理者および情報管理責任者は、報告のあった事故等について全て全学システム管理責任者またはシステム管理者に通知するとともに、必要な措置を直ちに講じなければならない。必要ならば、全学システム管理責任者に措置に関して指示または支援を要請すること。
- 全学システム管理責任者は、発生した全ての情報セキュリティ上の事故等に関する記録を一定期間保存し、最高情報セキュリティ責任者に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。
- 学内からの不正アクセスによって学外に被害を及ぼし、その事実関係の説明を被害者または第三者から求められた場合の対応手順を、規定として定めなければならない。

⑤ パスワード等の管理

- 教職員および学生は自己の保有するパスワードについて、不用意にもらしたりメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。
- 他の利用者のアカウントを使用してはならない。

5. 技術的セキュリティ

① 情報システムの管理

(1)情報システム管理記録の作成と管理

・ 情報管理責任者は、担当する情報システムにおいて行ったシステムの変更作業を記録し、適切に管理しなければならない。

(2)情報システム仕様書の管理

・ 情報管理責任者は、担当する情報システムの仕様書を最新の状態にしなければならない。また、システムの仕様変更等の処理行った場合は、その記録を作成しなければならない。

・ 情報管理責任者は、情報システムの仕様書を業務上必要とする者のみが閲覧できる場所に保管しなければならない。

(3)アクセス記録の取得

・ 情報管理責任者は、アクセス記録およびセキュリティ関連障害に関する記録を取得し、一定の期間保存しなければならない。

・ 情報管理責任者は、アクセス記録が窃取、改ざんまたは消去されないように必要な措置を講じなければならない。

・ 情報管理責任者は、可能な範囲でアクセス記録を分析しなければならない。

(4)障害記録の作成

情報管理責任者は可能な範囲で障害記録を作成し、一定の期間保存しなければならない。

(5)バックアップの取得

情報管理者は、重要性分類Ⅰ・Ⅱの行政情報については、外部媒体へのバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

(6)ソフトウェア導入に関する注意

教職員および学生は、本学の貸与したパソコンに業務上不必要なソフトウェアおよび出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。

(7)メールの送受信等

・ 教職員および学生は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。

・ 教職員および学生は、チェーンメールや不審なメールを他者に転送してはならない。

・ 教職員および学生は差出人が不明な、又は不自然なファイルが添付されたメールを受信した場合は、直ちに廃棄しなければならない。

(8)暗号化

・ 暗号化については、全学最高セキュリティ責任者が定める方法を用いなければならない。

・ 暗号のための鍵は、重要性分類Ⅰの情報として厳重に管理しなければならない。

(9)情報システムの入出力データ

・ 情報管理責任者は、情報システムに入力されるデータの適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

・ 情報管理責任者は、情報システムから出力されるデータの処理が正しく行われていることを確認しなければならない。

(10)業務目的以外の使用の禁止

教職員は業務目的以外での情報システムへのアクセス及びメールの使用を行ってはならない。

② 情報システムアクセス制御

(1)利用者登録

・ システム管理者は、情報システムの利用者の登録、変更、抹消等については、各情報システム毎に定められた方法に従わなければならない。

・ 利用者登録、変更等は、システム管理者に対する申請により行わなければならない。

(2)外部からのアクセス

外部からのアクセスの許可は必要最低限にしなければならない。

(3)外部ネットワークとの接続

- 外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成及び情報セキュリティレベル等を詳細に検討し、本学の情報資産に影響が生じないことを明確に確認した上で、全学セキュリティ責任者の許可に基づき接続しなければならない。
- システム管理者は、外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることのないようにセキュリティ対策に努めなければならない。
- 接続した外部ネットワークの情報セキュリティに問題が認められた場合には、情報管理者は、速やかに当該外部ネットワークを物理的に遮断しなければならない。
- 内部ネットワークの情報セキュリティに問題が認められた場合には情報管理者は速やかに当該内部ネットワークを外部ネットワークから遮断しなければならない。

(4)パスワード等の管理

- 情報管理者は、情報機器のID、パスワードを厳重に管理しなければならない。
- システム管理者は、ネットワーク並びにネットワーク上で利用される各種サービスのID、パスワードを適切に管理しなければならない。

③ コンピュータウイルス対策

(1)システム管理者は、次の事項を実施しなければならない。

- 情報システムのサーバ及び必要な機器にウイルス対策を行なうこと。
- ウイルスチェック用のパターンファイルは常に最新のものに保つこと。
- 定期的に新種のウイルスに関する情報収集や情報システム内部の感染状況等について情報収集をすること。
- コンピュータウイルス情報について、教職員に対する注意喚起を行うこと。
- コンピュータウイルスについて、教職員に対して必要な啓発活動を行うこと。

(2)教職員および学生は、次の事項を遵守しなければならない。

- 外部からデータ又はソフトウェアを取り入れる場合、及び外部に持ち出す場合には必ずウイルスチェックを行うこと。
- ウイルスチェックの実行を途中で止めないこと。
- 添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。
- システム管理者が提供するコンピュータウイルス情報を常に確認すること。

④ 不正アクセス対策

- システム管理者は、セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。
- システム管理者は、情報システムに不正な侵入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。
- システム管理者は、情報システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。

6. 運用

① 情報システムの監視

システム管理者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

② 情報セキュリティポリシーの遵守状況の確認

システム管理者及び情報管理者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じてないかについて確認を行わなければならない。

③ セキュリティ障害時の対応

セキュリティ障害が生じた場合には、システム管理者及び情報管理者は速やかに対応するとともに、再発防止の措置を講じなければならない。

(1)被害拡大の防止措置

- システム管理者は、故意の不正アクセス又は不正操作により情報システムに障害を及ぼす

ことが明らかな場合には、情報システムの停止を含む必要な措置を講じなければならない。
・ 情報管理者は、情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。

(2)障害の調査
・ 情報管理者は、セキュリティ障害が発生した場合、障害の発生を速やかにシステム管理者へ報告するとともに、次の項目について調査をしなければならない。
  ○ 障害の内容
  ○ 障害が発生した原因
  ○ 確認した被害、影響範囲
・ 調査した内容は速やかにシステム管理者に報告しなければならない。ただし、障害が軽度のものについては報告を要しないものとする。障害について調査、処理できない場合、システム管理者に対応を求めることとする。

(3)障害への対応
・ 情報管理者は、システム管理者の指示の下に速やかにセキュリティ障害を復旧し、その措置についてシステム管理者に報告しなければならない。
・ 障害が外部に重大な影響を及ぼすおそれがある場合には、システム管理者はすみやかに、最高情報セキュリティ管理者に報告のうえ必要な指示を仰がなければならない。

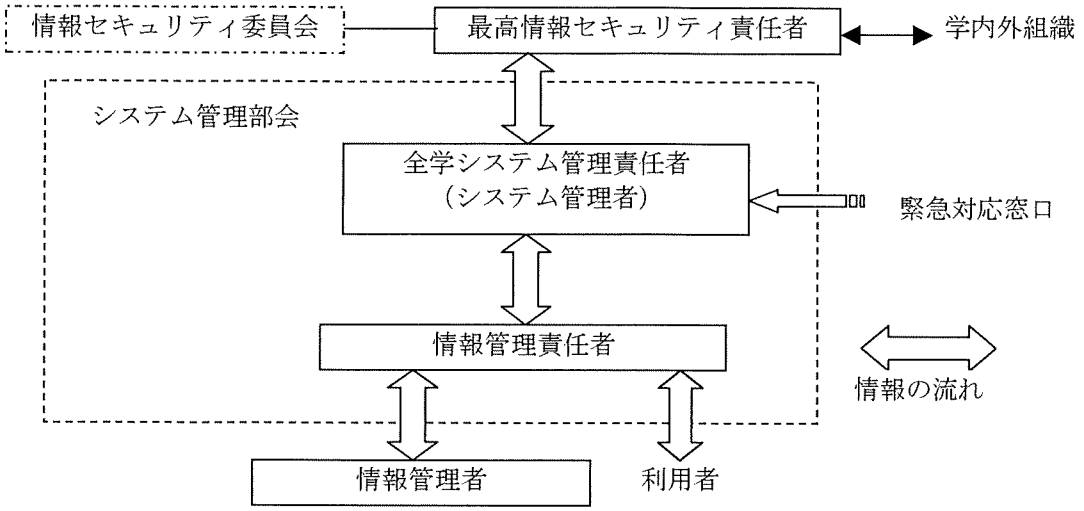
(4)再発防止の措置
システム管理者は、必要な再発防止の措置を講じるとともに、その結果を最高情報セキュリティ責任者に報告しなければならない。

7. 評価・見直し
・ システム管理者及び情報管理責任者は、当該部署の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じて改善措置を講じなければならない。
・ 最高情報セキュリティ責任者は、評価及び見直しが必要となる事象が発生した場合には、情報セキュリティ委員会に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

1. 管理体制

情報セキュリティ管理については、以下の体制とする

管理運用組織の構成



① 最高情報セキュリティ責任者：学長，（副）情報関係部門の長
- 全学の情報セキュリティに関する総括的な意思決定と、学内、他の組織および学外に対する責任を負う。

② 全学システム管理責任者：情報関係部門の担当者
- 全学の情報システム管理の実施に関し、緊急時の連絡など、総括的な対応に当たり、最高情報セキュリティ責任者を補佐する。

③ 情報管理責任者
- 情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う課（これに準ずるものを含む）に情報セキュリティに関する権限及び責任を有する情報管理責任者を置き、情報資産を取り扱う課、または学科の代表者をもってこれに充てる。
- 情報管理責任者は、所轄する情報資産に係る情報セキュリティ実施手順の作成・維持・管理を行うとともに、定められている事項について教職員に実施及び遵守させなければならない。
- 情報管理責任者は、使用する情報資産の機器や記録媒体について、第三者に使用させること、又は許可なく情報を閲覧させることがないように、適切な処置を施さなければならない。

④ 情報管理者
- 情報資産を現場で取り扱う担当者。

⑤ 情報セキュリティ委員会：最高情報セキュリティ責任者，全学システム管理責任者，情報管理責任者
- 情報セキュリティポリシーの策定、改訂を行なう。
- その他、情報セキュリティに関する重要事項の決定を行なう。